



and are not intertwined with the facts that the jury must decide - nor will they be more clear after trial proceedings.

The issue presented by the defense is whether the defendant's use of the secret chat feature in Telegram, when she was aware of the potential for investigation, would constitute conduct that an ordinary person would not consider to be criminal conduct. Determining this defense does not invade the province of the jury because the question of whether a charge is void for vagueness as-applied is a purely legal question. It does not require additional fact-finding. The critical facts are not in dispute. The defendant used the secret chat feature on Telegram and she was aware that, prior to the charged period, an online acquaintance was under investigation for immigration violations. After the defendant learned of the undercover's plans to travel, she told others that she had deleted everything from her phone out of fear of criminal prosecution.<sup>1</sup>

Likewise, contrary to the government's assertions, the viability of the defendant's as-applied challenge was not decided by *United States v. Kernell*, 667 F.3d 746, 756 (6th Cir. 2012) because *Kernell* specifically left open as-applied challenges to be determined on a case-by case basis. *Kernell* 667 F.3d at 755. The government is correct that the Court in *Kernell* found that the offense charged did not constitute void for vagueness as-applied because of the defendant's awareness of the potential for investigation. Unlike *Kernell*, however, the criminal conduct here does not involve destruction of records after the commission of a crime. Instead, the alleged destruction here takes place prior to the completion of any criminal act and involves measures that

---

<sup>1</sup> This statement does not cover the defense's argument that the use of the secret chat feature in Telegram should be struck as void for vagueness as-applied. Instead, this statement covers the alleged destruction of information on her phone which the defense did not challenge in its motion to dismiss because the statement is made almost a month after the defendant's last initiation of the secret chat feature with the undercover on September 30, 2018.

a normal person would use to protect their privacy (e.g. deleting their social media accounts and using the secret chat feature to prevent persons from distributing private statements they have made.)

This is not a distinction without a difference because ordinary people certainly would not realize that using standard features on popular and widely-used social media apps, and deleting their accounts on social media, could constitute a crime, even if they were worried about potential investigation in the future.

The government's final argument that there is no authority to show that applying § 1519 to the conduct here, actually makes the defense's point. The absence of authority buttresses the argument that this novel charging of § 1519 creates the potential for arbitrary and discriminatory enforcement. The government is clearly concerned about protective features that exist in social media to thwart government efforts at monitoring private speech and, as is the case here, is most likely to try to use § 1519 provisions to target individuals it perceives to be a threat to the government, as opposed to targeting ordinary criminal conduct. The defense urges the Court to reject this extension of § 1519 as did Judge Hollander in the context of sentencing in *United States v. Elshinawy*, 2018 U.S. Dist. LEXIS 51362 \*53 (D. Md. March 28, 2018).

Based on similar facts, Judge Hollander determined in *ElShinawy* that the use of the secret chat feature in Telegram and other encryption measures including: Surespot, TOR, proxy servers and VPNs to mask his online accounts during the planning and attempted commission of material support of ISIS, did not constitute obstruction of justice.<sup>2</sup> *Id.* Probation Services had recommended

---

<sup>2</sup> In addition to these measures, the defendant in that case also advised another conspirator to turn off the location tracking on his cell phone to avoid detection, directed another conspirator to delete their chats, and used a Linux-based operating system in such a highly sophisticated way

an obstruction of justice sentencing enhancement based on Application Note 4 to § 3C1.1 which includes "*destroying or concealing . . . evidence that is material to an official investigation . . .*". Nevertheless, Judge Hollander declined to apply the obstruction enhancement. In this case the defendant relies on *Elshinawy* for the proposition that the conduct put forth is sufficient for the court to determine whether, as a matter of law, Count Two fails as void for vagueness as-applied.

**B. The government's proffered conduct is insufficient to establish a nexus, as a matter of law, for Count Three.**

The government proffers that the conduct at issue in Count Three is the defendant's alleged attempt to corruptly persuade the undercover to destroy her phone and other contact information concerning the defendant prior to the undercover's surprise notice that she would be attempting to travel to Syria. The government argues that there is a sufficient nexus for Count Three based on: the defendant's alleged awareness that a woman she was in contact with was interviewed by the FBI; that in October 2018 another woman she knew was under investigation for possible immigration violations; that Telegram messages the defendant sent to an overseas contact in October 2018 stated that she "deleted everything" from her device so that she could say someone else used her phone to provide the contact information to the undercover; and that she made references to a potential prosecution, stating "One small mess up and I get 30 years", "I just don't want to go to jail for 30 years and leave my son in the hands of the Kuffar."

Even if true, these facts are insufficient to establish a nexus for obstruction of an official proceeding under either § 1512(b)(2)(B) or § 1512 (c)(1). *See United States v. Shavers*, 693 F.3d

---

that the FBI Staff Operations Specialist stated "there is no way to break into the LUX encryption." The defendant also used a "virtual machine" which the FBI Staff Operations Specialist explained deleted everything as soon it was closed and would then be erased forever, ensuring the defendant's activity was inaccessible. *Elshinawy*, 2018 U.S. Dist. LEXIS 51362 at \*54.

363 (3d Cir. 2012) (holding that the nexus requirement applies equally to both provisions of the statute.) The facts here are weaker than they were in the landmark case of *Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005). In *Arthur Andersen*, the defendant was well aware that the SEC had opened an informal investigation into Enron and that the investigation was likely to include documents in their possession. In advance of being subpoenaed, in-house counsel directed the employees to destroy documents that they were not required to retain regarding earlier audits. The Court specifically found that under these circumstances knowledge of a potential investigation was insufficient to create a nexus to knowingly obstruct an official proceeding and that it was not enough to show knowing intent to subvert or impede government fact-finding ability.

Here, like *Arthur Andersen* there is no nexus because at most, the evidence in October 2018 would indicate that if the undercover actually went to Syria, the defendant intended to have her take steps that would impede fact-finding in the future, rather than any particular proceeding. If such conduct was sufficient for a nexus, then there would have been no need for Congress to pass § 1519 in the wake of the *Arthur Anderson* case. The facts here are even stronger than in *Arthur Anderson* because, unlike *Arthur Anderson*, the alleged criminal activity had yet to be accomplished and, was instead, motivated by the defendant's desire not to be discovered in the event that the undercover followed through with her plan. Defensive conduct is not obstructive. *See Elshinawy*, 2018 U.S. Dist. LEXIS 51362 at \*53.

### **C. Conclusion**

For the reasons set forth above, the Defendant respectfully requests that this Court dismiss Counts Two and Three with prejudice, or in the alternative, defer judgement in accordance with Fed. R. Crim. P. 12(d).

Respectfully submitted this 17th day of July, 2020.

By: /s/ Charles D. Swift  
Charles D. Swift,  
*Pro Hac Vice* Attorney for Giampietro  
CLCMA  
833 E. Arapaho Rd., Suite 102  
Richardson, TX 75081  
(972) 914-2507

**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that on this 17th day of July, 2020, I electronically filed the foregoing Reply to the Government's Opposition to Motion to Dismiss Counts of the Indictment on Constitutional Grounds (Doc. 123) with the Clerk of the Court using the CM/ECF system which will send a notice of electronic filing to all counsel of record.

By: /s/ Charles Swift  
Charles D. Swift  
*Pro Hac Vice* Attorney for Giampietro  
833 E. Arapaho Rd., Suite 102  
Richardson, TX 75081